4. Other Techniques and Tools

Camilo Rocha
Escuela Colombiana de Ingeniería

7th International School on Rewriting (ISR2014)
Universidad Técnica Federico Santa María
August 25-29, 2014

The Maude-NPA

Maude-NPA is an analysis tool for cryptographic protocols that takes into account many of the algebraic properties of cryptosystems

- it supports the following algebraic properties
  - cancellation of encryption and decryption
  - Abelian groups (including exclusive-or)
  - exponentiation
  - homomorphic encryption
- the tool is similar to the original NRL Protocol Analyzer
  - it is based on narrowing
  - performs backwards search from a final state to determine whether or not it is reachable

Logical Model Checking

- Use of narrowing for
  - symbolic simulation of a rewrite relation
  - folding abstractions for reducing the symbolic search space
- K.Bae, J.Meseguer, and S.Escobar (WRLA 2014):
  - show folding abstractions can be faithful for safety LTL properties
  - show these abstraction methods can be used in combination and can be effective in making the logical state space finite
  - present the first narrowing-based LTL model checker

More information at

http://camilorocha.info

Thank you!